UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH ACCOUNT haris.m.fazal@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 22-mj-244-01-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Kyle D. Zavorotny, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since June 16, 2002. I am currently assigned to the Bedford, New Hampshire Resident Agency of the Boston Division of the FBI. I investigate federal crimes, including violations of

export-control regulations, and other offenses, including violations of Title 18 criminal statutes, to include 18 U.S.C. § 554, the Export Control Reform Act (50 U.S.C. § 4801 et seq.), and federal export regulations. I have received FBI training concerning computer-facilitated crime and other criminal activity. I am responsible for enforcing federal criminal statutes and am authorized to execute arrest and search warrants under the authority of the United States. During my tenure as a Special Agent, I have participated in the execution of numerous federal and state search warrants involving computers, documents, and electronically stored information, and I have written and assisted in the writing of search warrant affidavits.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested warrant, but does not set forth all of my knowledge about this matter. Statements attributed to individuals are paraphrased unless otherwise indicated.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 554, the Export Control Reform Act (50 U.S.C. § 4801 et seq.), and federal export regulations have been committed by Haris M. Fazal (also known as Haris Mahmood and/or Chaudhary Haris), Combine Communications, and others currently unidentified. There is also probable cause to search the information described in Attachment A for evidence and/or instrumentalities of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The FBI and the United States Department of Commerce - Office of Export Enforcement ("OEE") are conducting a criminal investigation regarding the activities of Haris M. Fazal, also known as Haris Mahmood and/or Chaudhary Haris ("Haris"), Combine Communications, and others currently unidentified, involving the unlawful export of goods from the United States. Haris is believed to be a citizen of Pakistan and to reside in the area of Lahore, Pakistan. Combine Communications is a business operating in Lahore, Pakistan. Haris represents himself to work for Combine Communications with the title of "Sales Engineer." The company is believed to be engaged in obtaining products manufactured outside Pakistan, including in the United States, for end use by entities within Pakistan.

7. The Export Control Reform Act of 2018 ("ECRA") provides, among its stated policy objectives, that "the national security and foreign policy of the United States require that the export, reexport, and in-country transfer of items, and specific activities of United States persons, wherever located, be controlled . . . ." Pub L. No. 115-232 § 752, 132 Stat. 2208 (2018). To that end, ECRA grants the President the authority "(1) to control the export, reexport, and in-country transfer of items subject to the jurisdiction of the United States, whether by United States persons or by foreign persons; and (2) the activities of United States persons, wherever located, relating to" specific categories of items and information. ECRA § 1753. ECRA further grants the Secretary of Commerce the authority to establish the applicable regulatory framework.

8. On or about September 2, 2020, a representative of a New Hampshire company received an e-mail from Haris, utilizing the name Haris M. Fazal and e-mail address

haris@combinecommunications.com. Haris identified himself as sales engineer for Combine Communications, and stated that the company was seeking certain blade antennas manufactured by the New Hampshire company for "a communications project for Pakistan Oilfields Limited." The blade antennas requested by Haris have various commercial and military applications, including avionics systems. Haris provided an address for Combine Communications of Suite #2, 4th Floor, Imtiaz Centre, Main Market, Gulberg, Lahore, and a cell number of +923334223283.

9. Officials of the New Hampshire company were aware that OEE was conducting other investigations regarding entities in Pakistan attempting to acquire the same blade antennas on behalf of certain entities listed on the Department of Commerce's "Entity List." Generally, the export of any product from the United States to a company on the Entity List requires a license issued by the Department of Commerce; moreover, there is usually a presumption of denial if any license application is made for an export to a company appearing on the Entity List. Based on this knowledge, the company officials felt the inquiry from Haris was suspicious. The FBI and OEE then opened the investigation referenced in paragraph 6.

10. As set forth on the relevant United States government website (bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list):

> [Commerce's Bureau of Industry and Security] first published the Entity List in February 1997 as part of its efforts to inform the public of entities who have engaged in activities that could result in an increased risk of the diversion of exported, reexported and transferred (in-country) items to weapons of mass destruction (WMD) programs. Since its initial publication, grounds for inclusion on the Entity List have expanded to activities sanctioned by the State Department and activities contrary to U.S. national security and/or foreign policy interests.

11. Based on my training and experience, I know that companies appearing on the Entity List seeking products manufactured in the United States will often use other non-listed

companies, commonly referred to as "front companies," as middlemen to hide the involvement of the listed companies in the transaction.

12. In other investigations, OEE has identified Pakistani company Advanced Engineering Research Organization ("AERO"), a company on the Entity List, as involved in attempts to acquire the blade antennas. The Entity List states that a license is required for export from the United States "for all items subject to the EAR [Export Administration Regulations]" to AERO, and there is a "[p]resumption of denial." The blade antennas are subject to the EAR.

13. An individual authorized by the company to communicate with potential customers ("Individual 1") exchanged e-mails with Haris. Haris made a second request for the same antennas, this time stating that the end user was the "Pakistan Airforce."

14. On or about November 21, 2020, Haris sent an e-mail in which he stated, "We have done business with … AERO. In fact, we have a couple projects already going on with these companies."

15. On or about March 2, 2021, Individual 1 called Combine Communications and asked to speak with Haris. The person who answered transferred the call to Haris. During this call, Haris stated that Combine Communications has a mix of government and private customers, but that the antennas requested would only be for "the government sector." He stated that the intended end user was "a military entity," and stated it was "the air force" to be used for "data links" on aircraft.

16. Haris inquired whether an "end user certificate" was needed. When told one was needed, Haris responded that he would discuss it with the customer, "because sometimes they're not very willing to share end user certificates." It was agreed that Individual 1 would send a blank standard Department of Commerce form (a BIS-711) to Haris.

17. Haris stated that they should "move forward cautiously but in Pakistan it gets tricky." When asked why, he stated "because there are a number of sanctions that have been placed on certain entities here," and that "there are … certain programs of Pakistan government that … we just have to be sure that we don't … make anyone notice."

18. Individual 1 asked Haris about his company's relationship with AERO. Haris stated that AERO is a "small department of the Air Force." He was asked if AERO was "the main customer here" and he answered yes, and when asked if there were "any other entities within the air force besides AERO we'd be dealing with," Haris said no.

19. On or about March 4, 2021, Individual 1 sent Haris a BIS-711 form and a questionnaire from the New Hampshire company requesting end use and end user information by e-mail.

20. Haris responded that he would "discuss this with the client and get back to you."

21. On or about March 9, 2021, Haris e-mailed the completed forms to Individual 1. The completed BIS-711 stated that the ultimate consignee for the purchase is "United Institute of Technical & Professional Education" located in Rawalpindi, Pakistan. It stated that the "antennas will be used on high performance car vehicles. The purpose is to obtain real time information of Engine Control Unit and different sensors placed inside the vehicle." It stated that the purchaser was "Technologic Enterprises." Neither AERO nor Combine Communications appeared on the form.

22. On or about March 24, 2021, Individual 1 called Haris. Haris was asked why the form listed the United Institute of Technical and Professional Education as the ultimate consignee, rather than AERO, as Haris had stated in the earlier call that AERO was the customer. Haris stated that "they don't want to put it in their own name" and "[t]hey don't give end user

certificates." He stated that the United Institute is "one of their front companies." Individual 1 expressed concern that the activity was illegal, and Haris stated that he understood. Haris stated that Technological Enterprises, listed as "Purchaser" on the BIS-711, was a "facilitator"; Combine Communications would import the items, send them to Technological Enterprises, and Technological Enterprises would provide the products to AERO.

23. Individual 1 asked Haris about the statement on the form that the products would be used on race cars, stating "we both know it's going on a plane right?" Haris laughed and stated "[y]es sir we both know that" and agreed that the statement did not make sense. Haris stated that he is an electronics engineer, and that the parameters listed "makes them not make sense to anyone who understands antennas."

24. Individual 1 asked Haris "we're violating the law and we're exporting something that shouldn't be exported. Have you ever done this before?" Haris replied "Yes we have done this."

25. Haris agreed to "have the forms refilled and … make it look legit" and recontact Individual 1.

26. On or about April 6, 2021, Individual 1 called Haris. Haris stated that AERO would not use its name on the forms, and that he had been assured that the United Institute of Technical and Professional Education, listed as ultimate consignee on the BIS-711, would not be "flagged" by the U.S. Department of Commerce. He stated that he had not yet had an opportunity to discuss the description of the end use with AERO.

27. Haris agreed with a statement that the United Institute is a "front company for AERO" and stated "[a]ll the procurement that we do for AERO, we do through front companies."

28. On or about May 14, 2021, Haris sent an e-mail to Individual 1 stating that his client had obtained the antennas from another source and he was no longer seeking these products.

29. On or about May 17, 2021, Haris sent Individual 1 a link to his LinkedIn social media profile. This profile lists his name as "Haris Mahmood."

30. On or about February 2, 2022, a North Carolina company contacted the Department of Commerce regarding an order that the company felt was suspicious. The order came from an individual using the name Haris Mahmood, representing Combine Communications, and provided a physical address for the company of Imtiaz Centre Main Market Gulberg, 4th Floor, Lahore 54000, Pakistan (substantially the same as the address provided by Haris in the September 2020 product requests) and the same telephone number utilized by Haris. The order requested an aircraft tire gauge to be shipped to an address in Illinois, but Mahmood stated that he was located in Pakistan. The e-mail "from" line bore the name "Chaudhary Haris." The e-mail came from a Gmail account, chharis999@gmail.com, and the sending internet protocol (IP) address was located in Pakistan.

31. The North Carolina company asked for the end user of the product, and Haris Mahmood replied "Airborne Aviation, Lahore, Pakistan." The company asked additional questions, and Haris Mahmood replied that he is in Pakistan, that the Illinois address "is my freight forwarder," and that "Chaudhary Haris is Haris Mahmood. I am the same person."

32. The LinkedIn profile provided by Haris (described in paragraph 29 above) was viewed on February 2, 2022, and the e-mail address listed in his "Contact Info" section is chharis999@gmail.com, the same as that used to contact the North Carolina company.

33. Based on the information above, on April 6, 2022, this Court issued a search warrant directed to Google for communications and stored files associated with the Google account chharis999@gmail.com. In response to the warrant, Google provided, *inter alia*, files stored in a Google Drive account, which appear to be backups of computers or other electronic devices used by Haris.

34. Among the files was a pdf document from RBC Royal Bank showing a confirmation for a payment to an aviation supply company located in Oklahoma. Investigators contacted the aviation supply company and requested information regarding the transaction that resulted in the payment from RBC Royal Bank. The company provided documents showing that on or about February 4, 2022, Haris, using the email address haris.m.fazal@gmail.com, communicated with the company regarding the purchase of an aviation tool kit. Haris completed the purchase and the tool kit was shipped to the same Illinois address mentioned above. Haris inadvertently paid twice for the order, and requested that the overpayment be refunded via check sent to an individual at Stony Brook University in Stony Brook, New York.

35. Thus, there is probable cause to believe that Haris uses the haris.m.fazal@gmail.com account in furtherance of his business of importing aviation equipment on behalf of the Pakistani government—the same line of business that led Haris to commit attempted violations of 18 U.S.C. § 554, the Export Control Reform Act, and federal export regulations.

36. Based on my training and experience, I know that individuals involved in attempts to acquire United States-manufactured products from outside the United States frequently utilize e-mail to contact companies to request quotes, provide specifications, and place orders; Haris has utilized the subject account to order a product from a United States company.

BACKGROUND CONCERNING GOOGLE AND E-MAIL

37. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("e-mail") access, to the public. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

38. A Google subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

39. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I

know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

40. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

41. In general, an e-mail that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Google's servers for a certain period of time.

42. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider

or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

43. As explained herein, information stored in connection with an e-mail account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an e-mail account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the e-mail provider can show how and when the account was accessed or used. For example, as described below, e-mail providers typically log the Internet Protocol (IP) addresses from which users access the e-mail account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the e-mail account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via e-mail). Last, stored electronic data may provide relevant insight into the e-mail account owner's state of mind as it relates to the offense under investigation. For example, information in

the e-mail account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

44. Based on the forgoing, I request that the Court issue the proposed search warrant.

45. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the execution of this warrant. The government will serve the warrant on Google, which will then compile the requested records at a time convenient to it. Thus, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

46. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from

prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

/s/ Kyle D. Zavorotny
Kyle D. Zavorotny
Special Agent
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: **Nov 21, 2022**
Time: **3:34 PM, Nov 21, 2022**

Honorable Andrea K. Johnstone
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with e-mail address haris.m.fazal@gmail.com and all associated accounts that are stored at premises owned, maintained, controlled, or operated by Google LLC, an electronic communications service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 9, 2022, the Provider is required to disclose the following information to the government for the account or identifier listed in Attachment A:

a. The contents of all e-mails, from September 1, 2020 to the date of execution, associated with the e-mail address haris.m.fazal@gmail.com, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the e-mail and associated accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account(s) was/were created, the length of service, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the e-mail and associated accounts, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the e-mail address and/or associated accounts, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 554, the Export Control Reform Act (50 U.S.C. § 4801 et seq.) and/or other export regulations, those violations involving Haris M. Fazal, also known as Haris Mahmood or Chaudhary Haris, Combine Communications, and others currently unidentified, including information pertaining to the following matters:

(a) Records of communications involving the identified e-mail account relating to the purchase and sale or attempted purchase or sale of any items manufactured and/or sold by companies or individuals in the United States, including, but not limited to, requests for quotes, orders, invoices, payment information and shipping information; communications between the identified e-mail account and US based freight-forwarding companies or individuals acting in such a capacity; communications between the identified e-mail account and end users and/or intermediate consignees of items sought or potentially sought for purchase; and communications between the identified e-mail account and other employees or officials of Combine Communications.

(b) Evidence indicating how and when the e-mail account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the e-mail account owner;

(c) Evidence indicating the e-mail account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the user(s) of the account about matters relating to the violations described above, including records that help reveal their whereabouts.